HUMBOLDT-UNIVERSITÄT ZU BERLIN
RECHENZENTRUM

Humboldt-Universität zu Berlin • Rechenzentrum • Unter den Linden 6 • D-10099 Berlin

Computerviren

Erkennung, Beseitigung, Vorsorge

Kursunterlagen

Autor: Lutz Stange
Telefon: 2093 2329
E-Mail: stange@rz.hu-berlin.de
WWW: http://www.rz.hu-berlin.de/rz
Stand: November 2002

Inhalt:

Literaturhinweise:

Zentren für Virensupport:
- http://agn-www.informatik.uni-hamburg.de/vtc/dt1.htm
- http://agn-www.informatik.uni-hamburg.de/avlinks/avlinks.htm
- http://www.tu-berlin.de/www/software/hoax.shtml (auch http://www.hoax-info.de)
- http://www.uni-siegen.de/security/viren/index.html
- http://www.datarescue.com/other.htm
- http://ciac.llnl.gov/ciac/CIACHoaxes.html
- http://www.bsi.de
- http://www.percomp.de/virusinformationen.html
- http://www.heise.de/ct/antivirus/

Empfehlungen für die HU:
- http://www.hu-berlin.de/rz/rzmit/rzm15/6.html
- http://www.hu-berlin.de/rz/viren/index.htm
- http://www.hu-berlin.de/rz/vwedv/empfehlg/empf_vir.html
- http://www.hu-berlin.de/rz/vwedv/empfehlg/minst.html

Firmenangebote:
- perComp-Verlag GmbH: http://www.percomp.de/
- F-Prot: http://www.complex.is/cgi-bin/home_pager
- Network Associates (NAI): http://www.nai.com/
- Symantec: http://www.symantec.com/avcenter/
- BlueMerlin: http://www.bluemerlin-security.de/
- DataFellows: http://www.Europe.DataFellows.com/virus-info/

1 Viren als selbstreproduzierende digitale Wesen

In der Biologie ist ein Virus ein Krankheitserreger, der keinen eigenen Stoffwechsel besitzt. Er greift statt dessen eigenständige Zellen an, nistet sich in ihnen ein und programmiert die DNA-Erbinformation der Wirtszelle um. Damit ist die Analogie schon erschöpft. Ein Computervirus ist einfach ein Stück Software, das sich ein Programm sucht und seinen Programmcode dort ablegt. Gelangt das Wirtsprogramm zur Ausführung, kann der Virus aktiv werden, indem er z. B. Daten löschen oder ändern, Arbeitsabläufe stören, E-Mails versenden, den Absturz des PCs bewirken oder sich fortpflanzen, d.h. sich selbst kopieren kann.

> Ende 1996 gab es etwa 10.000 Computerviren, zwei Jahre später sind es bereits über 20.000.
> Heute sind über 60.000 solcher Computerviren bekannt und täglich kommen bis zu 15 neue hinzu.

Computer-Viren sind inzwischen bei nahezu jeder EDV-Nutzung ein heißes Thema. Allgemeiner spricht man von **Malware** oder **Malicious Code**, womit auch andere, absichtlich schadenverursachende Programme eingeschlossen sind, die sich im Gegensatz zu Viren (i.A.) nicht selbsttätig replizieren.

Eine mögliche **Definition**:

> Viren sind destruktive Programme, die andere Programme verändern können, wobei es eine Kopie von sich selbst einfügt, sich somit von Datenträger zu Datenträger kopieren können und Schäden an Daten, Programmen, Rechnerkonfigurationen und Arbeitsabläufen verursachen können.

Das Ausmaß von Schäden durch Computerviren reicht von einfachen Bildschirmanimationen bis zur Zerstörung aller Programme und Daten auf Disketten und Festplatten. Programmviren verändern Programmdateien, so dass nach einer Infektion keine Aussage über die Zuverlässigkeit des infizierten Programms gemacht werden kann. Ein von einem Virus infiziertes Programm kann i.d.R. nicht mehr fehlerfrei ablaufen. Häufig bemerkt der Benutzer einen Fehler nicht sofort, sondern erst später, wenn er den fehlerhaften Programmteil benutzt. Einige Computerviren stören gezielt den Arbeitsablauf am Computer.

Ein **Rückblick**:

1949	Theorie von selbstreproduzierenden Automaten (John von Neumann)
60er	Erste Programme mit (gewollter) Selbstkopie zur Arbeitsorganisation (Wiedereinreihen an das Ende einer Warteschlange)
	Core Wars: erstes Computerspiel mit dem Ziel, kostbare Rechenzeit zu stehlen
70er	Creeper: erstes Programm mit unkontrollierter Fortpflanzung im ARPANET
	Reeper: Programm zur Verfolgung und Ausschaltung von Creeper
1981	Erstes Auftauchen des Virus-Begriffes
1984	Dissertation von Fred Cohen zu Viren
1985	Veröffentlichung des Quellcodes für einen Virus für den Apple II
1986	erste in Umlauf gebrachte Viren (PAKISTANI BRAIN für DOS)
1989	erste polymorphe Viren
1990	erste Virus Construction Kits
1992	erste große Hysterie durch den Michelangelo-Virus
1995	erste Makro-Viren
1999	erste Skript-Viren

Viren bestehen im wesentlichen aus drei Komponenten:

- Komponente zur Vermehrung/Ausbreitung
- Komponente zur Tarnung

- Komponente mit Schadensfunktion

Neben verschiedenen Varianten gibt es vier große Gruppen von Viren, die uns das Leben schwer machen:

- Dateiviren,
- Bootsektorviren,
- Makroviren,
- Skriptviren.

> Das Phänomen der Computerviren, dieser selbstreproduzierenden digitalen Wesen, wird in der Öffentlichkeit seit den frühen 80er Jahren wahrgenommen. Die ersten Versuche in diese Richtung wurden im Rahmen akademischer Forschungen entwickelt. Die Programme hatten keinen eigentlichen Zweck, wenn nicht den einer geistigen Herausforderung, eines Experiments. Der Computervirus reihte sich in den Diskurs des ewiger Menschheitstraums von den „intelligenten Maschinen" ein und wurde in den entsprechender Sparten der Wissenschaft nach den Prinzipien des künstlichen Lebens (artificial life) weiterentwickelt Hieraus ergab sich die Analogie zu den Prinzipien biologischer Viren. Der Hauptimpuls zu Entwicklung der unterschiedlichen Viren seitens einzelner Programmierer lag zum Teil bestimmt auch darin, die Neugier zu befriedigen, die undurchsichtige Topologie des Internets auszuloten - was passiert, wenn ...
>
> aus: „I love you - Computer, Viren, Hacker, Kultur"
> Eine Ausstellung von digitalcraft, Frankfurt/M., 23.5. - 13.06.2002

Computerviren gibt es praktisch auf allen gängigen Rechner- und Betriebssystemplattformen: DOS, Windows (alle Versionen), Mac OS, Unix inkl. Linux, aber auch auf Netz-Servern (Windows NT/2000/.NET, Novell Netware, Unix u.a.). Drei neue Gefahrenquellen waren in den letzten vier/fünf Jahren auszumachen, die in ihren Auswirkungen die konventionellen Computerviren in den Schatten stellen: Makroviren, Skriptviren und Netzviren.

Makroviren:
Makroviren haben zweifellos eine neue Ära in der Virenprogrammierung eingeläutet. Das hat verschiedene Ursachen: Zum einen hat keiner mit solchen Viren gerechnet, zum anderen ist er äußerst leicht herzustellen. Schon mit einfachen Grundkenntnissen der Makrosprache ist jeder Anwender dazu in der Lage. Es gibt sogar schon Makroviren-Baukästen, mit welchen das dialog- und fensterorientiert und fast ohne Programmierkenntnisse möglich ist. Weiterhin stellt er sowohl weltweit als auch bei uns im Hause von der Häufigkeit des Auftretens her die größte Gefahr dar.
Makroviren betreffen Anwendungen, die über eine eigene Makrosprache verfügen. Vielfach sind Microsoft Office Programme davon betroffen.
Makroviren sind plattformübergreifend: Bei Verfügbarkeit der entsprechenden Anwendung können sie durchaus z. B. von einem Windows-Rechner auf einen Apple Macintosh übertragen werden. Schließlich besteht die neue Qualität darin, dass der Virus nicht durch die Ausführung von Programmen aktiv wird, sondern durch die bloße Benutzung von Daten, von Resultaten der Anwendungsprogramme. Das erschwert den Schutz vor Verbreitung dieser Viren.

Skriptviren:
Skriptviren greifen auf die Programmiersprachen Visual Basic Script (VBS) und JAVA zurück. Dabei werden Viren auf der Basis von Visual Basic Script insbesondere auf dem und durch den lokalen Rechner aktiviert. JAVA- und VBS-Viren können ihre Schadensfunktion durch die Arbeit mit aktiven Web-Seiten ausführen.
Skriptbasierte Viren (und Würmer) sind vor allem deshalb so populär, weil sie auch von weniger erfahrenen Personen leicht zu schreiben und dennoch sehr effektiv und zerstörerisch sind. Fast alle gängigen Würmer arbeiten sogar mit Beispielcode, der direkt von Microsofts Web-Seiten stammt. Die dominierende Verbreitung der Windows-Betriebssysteme und Office-Programme

wie Outlook, Word und Excel liefert eine wohlbekannte Plattform für die Virenautoren und garantiert, dass die schädliche Wirkung bei möglichst vielen Opfern eintritt.
Oft besteht bei Anwendungen der Irrglaube, dass durch E-Mails nur die Benutzer von Outlook gefährdet seien. Tatsächlich kann jedoch jedes E-Mail-Programm, das Dateianhänge verwaltet, auch die schädlichen Komponenten eines Wurms übertragen. Jeder Mail-Client, der HTML-Code und aktive Inhalte (besonders unter Zuhilfenahme des Internet Explorers) auswertet, läuft Gefahr, riskante Befehle bereits in der Vorschau oder beim Lesen von Nachrichten auszuführen.

Netzviren:
Netzviren sind keine eigene Virenart, sie zeichnen sich nur durch die Besonderheit der Infektion aus: Während in der Vergangenheit nur durch das Einlegen und Benutzen von verseuchten Datenträgern eine Übertragung möglich war, bietet das Computernetz heute ganz neue Mechanismen für ihre Verbreitung. Bei der Nutzung von Diensten des Internets sollte man sich praktisch bei jedem Zugriff Gedanken über eine mögliche Virenverseuchung des eigenen Rechners machen.
Eine neue Qualität der Netzviren stellen diese dar, die automatisch Funktionen in Mail-Programmen aktivieren und so für die Verbreitung sorgen. D.h. eine Fortpflanzung findet nicht nur durch das explizite Versenden einer Mail mit verseuchtem Attachment statt, sondern schon durch das unbewusste Aktivieren des Virus.

> Viren sind ein Manifest der Genialität, sich selbstreproduzierende Wandgemälde mit der Fähigkeit zu reisen und vom Können ihres Schöpfers zu kunden.
>
> Massimo Ferronato

Die Gefahren der Netzviren werden sich in Zukunft noch verschärfen und allmählich auf drahtlose Systeme übergreifen. Durch den Trend hin zur mobilen Kommunikation entstehen völlig neue Plattformen und Netzwerke, parallel dazu entwickeln sich auch neue Bedrohungen. Erste Sicherheitsvorfälle sind in diesem Bereich bereits aufgetreten.

Antiviren-Unternehmen

Andere 5%
Computer Associates 5%
Trend Micro 12%
44%
Symantec 34%

Im Jahr 1999 verkauften Hersteller von Antiviren-Software Produkte im Wert von 785 Mio. Dollar.
(Quelle: Gartner Dataquest Aug. 2000)

2 Virenarten und -varianten

In diesem Abschnitt werden einige Begriffe erläutert, die im Umfeld von Malware eine Rolle spielen. Computerviren lassen sich meist nicht eindeutig einer der hier beschriebenen Arten und Varianten zuordnen. Meist treten sie in Mischformen auf, d.h. sie lassen mehrfach klassifizieren. Natürlich sind neben dem Auftauchen neuer Viren auch ganz neue Arten von Virenklassen nicht auszuschließen. Zusätzlich werden an dieser Stelle auch Klassen von Malware beschrieben, die den Viren-Begriff im klassischen Sinne überschreiten, im Zusammenhang des Umgangs mit dieser Problematik aber eine wichtige Rolle spielen.

Dateiviren (Programmviren, COM-Viren)
Dateiviren infizieren ausführbare Programme (COM-, EXE-, OVL-, OBJ-, SYS-, BAT-, DRV-, DLL-Dateien) und können bei deren Abarbeitung aktiviert werden.

Bootsektorviren (Bootviren)
Bootsektorviren verstecken sich im Bootsektor von Festplatten und Disketten sowie im Master Boot Record (MBR) von Festplatten, können sich nach dem Booten von eben diesem Datenträger resident in den Hauptspeicher verlagern und permanent Schaden anrichten.

Makroviren
Makroviren sind in Makros (d.h. in automatischen Programmabläufen) von Dokumenten, Tabellen, Grafiken, Datenbanken u.a. enthalten. Sie können bei Weiterverarbeitung dieser Dateien mit den entsprechenden Anwendungsprogrammen (z.B. Word für Windows) aktiv werden.

Hybridviren (Multipartite Viren)
Hybridviren sind Kombinationen von mehreren Virenarten. Damit machen sie sich verschiedene Ausbreitungsmethoden gleichzeitig nutzbar und sind somit schwerer aus dem System zu entfernen. Sie vereinen oft Virenmethodik mit Hackerangriffen und besitzen dadurch ein noch höheres Schadenspotenzial.

Skriptviren
Eine ganz neue Generation von Viren sind neben den schädlichen JAVA-Applets vor allem die auf Visual Basic Skript basierenden Skriptviren. Diese können in VBS-Dateien und sogar in HTML-Code versteckt sein.

Linkviren
Linkviren (auch: Directory-Viren) manipulieren die Datenträger-Einträge so, dass vor dem Aufruf von bestimmten Programmen zuerst andere Teile des Datenträgers angesprungen werden, welche den eigentlichen Virencode enthalten.

Stealth-Viren (Tarnkappenviren)
Stealth-Viren sind Viren mit speziellen Mechanismen, sich vor Virensuchprogrammen zu verstecken. Sie können z.b. eine infizierte Datei vor der Überprüfung restaurieren und somit die Verseuchung unkenntlich machen.

Polymorphe Viren
Polymorphe Viren verändern in einem bestimmten Rhythmus ihr Aussehen, so dass sie für Virenscanner, die nach Erkennungsmustern arbeiten, nicht oder schwer entdeckt werden können.

Slow-Viren
Slow-Viren sind Viren, die lange Zeit unentdeckt bleiben, weil sie die Daten nur geringfügig manipulieren. Damit wird es wahrscheinlich, dass sie auch auf Sicherungsdatenträger übertragen werden, so dass der Benutzer keine virenfreien Duplikate oder älteren Versionen mehr zur Verfügung hat.

Experimentelle Viren
Experimentelle Viren treten, wenn überhaupt, nur im Bereich der LISP-Programmierung auf und infizieren dabei den Quellcode. Sie sind allerdings sehr schwer zu programmieren und finden in der „normalen“ PC-Welt kaum Beachtung.

Würmer
Würmer sind keine Viren im eigentlichen Sinne, da sie keine Wirtsprogramme benötigen, sondern ausschließlich sich selbst kopieren.

Trojanische Pferde
Trojanische Pferde (Trojaner) sind auch keine Viren im eigentlichen Sinne (da sie sich i.d.R. nicht selbst reproduzieren), sondern Programme mit Virenfunktionalität, die sich hinter dem Namen von bekannter (harmloser) Software verstecken. Der Begriff Trojaner wird oftmals synonym für Spionage-Software verwendet. Besondere Kennzeichen sind, dass sie oftmals lange Zeit unentdeckt bleiben und von „innen nach außen“ wirken.

Hoax
Ein Hoax ist eine (per Mail) versandte Warnung vor einem imaginären Computervirus. Vielmehr sind diese Warnungen selbst als Malware einzustufen, da sie erheblichen Schaden anrichten können. Kettenbriefe gehören auch in diese Rubrik.

Logische Bomben
Logische Bomben sind Programme, die beim Eintreten bestimmter Umstände (Erreichen eines Datums, Löschen eines speziellen Datensatzes einer Datenbank, Erzeugen einer Datei mit einem speziellen Namen) Schaden anrichten können.

Direct-Action-Viren
Direct-Action-Viren infizieren bei der Ausführung des infizierten Programms sofort weitere Programmdateien und führen eine eventuell vorhandene Schadensroutine sofort aus. Anschließend übergibt der Virus die Kontrolle an das ursprüngliche Programm und entfernt sich aus dem Hauptspeicher.

ANSI Viren
ANSI Viren sind im eigentlichen Sinne keine Viren, sondern nur besonders „reizende“ Manipulationen der Funktionstasten mit ANSI-Zeichenketten. Sie können nur dann Schaden anrichten, wenn der Treiber ANSI.SYS geladen wurde.

Denial-Of-Service (E-Mail-Bombing)
Beim E-Mail-Bombing überhäuft ein Angreifer ein Zielsystem mit Mails, so dass im Extremfall die normale Nutzung von Mail nicht mehr möglich ist.

E-Mail-Viren
E-Mail-Viren sind Viren, die sich im Attachment von Mails verstecken und die sich bei deren Benutzung auf den lokalen Rechner übertragen.

Tastatur Keylogger
Tastatur Keylogger sind Programme, die der Protokollierung von Tastatureingaben dienen. Damit ist es möglich, geheim zu haltende Eingaben, wie Passwörter, Sicherheitscodes usw. auszuspionieren.

Sendmail Bugs
Sendmail Bugs sind trojanische Pferde, die in das zum Verschicken von E-Mails wichtige Sendmail-Programm eingeschmuggelt werden und Passwörter ausspionieren.

DNS-Angriff
Bei einem DNS-Angriff erfolgt eine Umleitung einer Internet-Anfrage eines Nutzers an einen Rechner auf einen dritten Rechner. Auf diese Weise können z.B. Passwörter ausspioniert werden.

RIP-Angriff
Die gesamte Kommunikation zwischen zwei Rechnern wird zu einem externen Angreifer umgeleitet und ausspioniert. Danach werden die Daten dem richtigen Adressaten zugestellt.

Backdoors
Backdoors (Hintertüren) lassen z.B. eine Fernsteuerung des Rechners zu. Damit kann ein Angreifer von außen über das Netzwerk Daten manipulieren oder ausspionieren.

Keystroke Reader
Jeder Tastendruck eines Benutzers wird durch ein in den Rechner eingeschmuggeltes Programm heimlich mitgelesen und aufgezeichnet. Dadurch lassen sich Passwörter ausspionieren.

Packet Sniffer
Packet Sniffer sind Programme, die von Benutzern ausgesendete Daten lesen und Passwörter erkennen und sammeln können.

IP Spoofing
Ein Angreifer erzeugt Datenpakete mit gefälschter Absenderadresse; der Empfänger-Computer nimmt an, einen internen Nutzer vor sich zu haben, und gibt Zugangsrechte frei.

ICMP-Angriff
ICMP-Protokolle dienen der Fehlermeldung und automatischen Reparatur bei Netzwerkproblemen. Gefälschte ICMP-Protokolle können die Funktionsfähigkeit von Netzwerken beeinträchtigen.

Frage: Ist an den Warnungen vor Viren in E-Mails („Good Times“, „Penpal Greetings“, „Win A Holoday“ usw.) etwas dran?

Antwort: Nein! Es tauchen im Internet immer wieder Warnungen auf, dass Viren als E-Mail verschickt würden, die allein durch das Lesen der Mail aktiviert würden. Technisch ist das allerdings unmöglich. Diese Art Mails heißen **HOAX** und sind eher unter der Rubrik E-Mail-Bombing zu erfassen. Etwas anderes sind Attachments, die virenbehaftet sein können.

Beispiel:
> > > Subject: Viruswarnung bitte lesen!
> > >
> > > Betreff: Achtung Virusmeldung bitte lesen!
> > >
> > > Von: Polizei Baden-Württemberg [mailto:webaster@polizei-bw.de]
> > > Bitte weiterleiten, an alle Personen die Sie kennen und Internet-Zugang haben.
> > > Vielleicht erhalten Sie per Mail einen Bildschirmschoner ‚Budweiser’ in einer Datei ‚buddylyst.zip’
> > > AUF KEINEN FALL ÖFFNEN!!!!!!! Gleich löschen
> > >
> > > Wenn Sie diese Datei entpacken, verlieren Sie alle Daten auf Ihrem Computer, die Festplatte wird
> > > komplett zerstört und die Person, die Ihnen diese E-mail geschickt hat, erhält Zugang zu Ihrem
> > > Internet-Namen und Passwort. Dieser Virus ist seit gestern im Umlauf und sehr gefährlich.
> > >
> > > Mailen Sie an alle Personen aus Ihrem Adressbuch diese Warnung.
> > > AOL hat bestätigt, dass er sehr gefährlich ist und dass noch kein Antivirenprogramm existiert,
> > > das ihn zerstören könnte. Bitte leiten Sie diese email weiter an Ihre Kollegen, Bekannte, Freunde

Das ist **keine** Viruswarnung!

3 Virenbefall und -erkennung

Obwohl Computerviren ein Problem darstellen, sollte ihre Bedeutung nicht überbewertet werden. Die häufigste Ursache für ein „nicht ordnungsgemäßes Funktionieren“ des Computers sind **Benutzerfehler**, gefolgt von **Hardwarefehlern** und **Softwarefehlern**. **Viren** kommen erst an vierter Stelle.

Computer-Viren stehen mit 64 Prozent auf Platz eins der Sicherheitsverletzungen.

Bei dem Eintreten eines der folgenden Ereignisse bzw. in einer der folgenden Situationen kann man als Ursache einen Virenbefall nicht ausschließen:

- „ungewöhnliche“ Verhaltensweise und Reaktionen des Computers
- Auftreten von Datenverlust und/oder Datenverfälschung
- Meldungen eines Virentest-Programms
- Warnungen anderer Programme und/oder des Betriebssystems
- Veränderungen an Dateien und/oder Datenträgern
- Veränderung der Größe und/oder des Datums der letzten Änderung von Dateien
- heftiges Arbeiten der Festplatte, ohne dass etwas geladen oder gespeichert wird
- es steht weniger Arbeitsspeicher als bisher zur Verfügung
- ungewöhnlich lange Zeit für einen Programmaufruf bzw. allgemein Geschwindigkeitsverlust
- Programme verschwinden oder neue tauchen auf
- Ausschriften des Virus
- Erfahrungen (☺!)

Frage: Können E-Mails Leben retten?

Antwort: Nein! Je unglaubwürdiger der Inhalt, desto größer die Verbreitung. Kettenbriefe überschwemmen das Internet.

Beispiel:

>>>Dieser Bericht enthält eine Bitte: Könnt ihr so gut sein, diese Mail weiterzuleiten? Dadurch könnt ihr einem kleinen Jungen (Brian) aus Buenos Aires helfen. Brian hat mit einer schweren Erkrankung an seinem Herzmuskel zu kämpfen und wartet dringend auf eine Transplantation. Doch es gibt ein "Aber": Diese Operation kostet 115.200 US Dollar. Der ISP (Internet Service Provider) bezahlt 0,01 Dollar für jede Mail, die für diesen Zweck versendet wird und mit dem Titel: "Solidarida con Brian" über den Server gehen. Es ist wichtig, schnell zu handeln! Neben Brians Krankenbett steht ein Notebook mit Modem um zu zählen. Es sind 11,5 Mill. Mails nötig, um die Operation finanzieren zu können. Könnt ihr, wenn möglich, an jeden den ihr kennt, eine Kopie von dieser Mail senden? Das kostet max. 2 Minuten eurer sicherlich kostbaren Zeit, während es für Brian lebenswichtig ist. Zerstöre die Kette bitte nicht und vergesse vor allem nicht den Titel "Solidarida con Brian", der unter Subjekt/Betreff stehen muss, denn das ist die Kontrollmöglichkeit des Servers. Vielen Dank im Namen von ida van Kampen-Damsma und Betty Meyboo de Jong, Hochschullehrerinnen für Allgemeinmedizin an der Rjks Universität in Groningen. Tipp: Kopiere diesen Bericht und forwarde ihn an dein ganzes Adressbuch. Und noch was: Diese Mail wurde von einer Schülerin aus Deutschland am 9.2.2002 wieder leserlich gemacht, weil durch das weitersenden lauter >>>> in der Mail waren. Also, wenn ihr die Mail weitersendet, drückt bitte nicht einfach auf weiterleiten, sondern kopiert sie in eine neue Mail, damit sie leserlich bleibt. Wenn ihr sie weiterschickt, entfernt bitte auch die Werbung der Freemail-Anbieter ganz unten in der Mail. Danke!!! Solidarida con Brian <<<

4 Virenerkennung und -beseitigung

4.1 Antivirensoftware

4.1.1 Was leistet Antivirensoftware?

Es gibt mehrere Arten von Algorithmen für Antivirensoftware (Virenscanner):

- Ein **Virensuchprogramm** ist ein Programm, das nach bekannten Viren sucht. Da laufend neue Viren auftreten, müssen Suchprogramme regelmäßig aktualisiert werden.
- Ein **heuristisches Programm** verfügt über Methoden, auch bisher unbekannte Schädlinge aufzuspüren. Dazu gehören das Erkennen typischerweise verwendeter Codesequenzen und Programmlogik.
- Ein **Prüfsummenprogramm** erkennt Änderungen an Dateien. Es berechnet für jede zu schützende Datei eine eindeutige numerische Prüfsumme. Das Prüfsummenprogramm kann dann die Prüfsumme einer Datei erneut berechnen, so dass Abweichungen erkannt werden. Ausführbare Dateien ändern sich im Allgemeinen nicht; wenn also die neu berechnete Prüfsumme von der ursprünglichen Prüfsumme abweicht, ist möglicherweise ein Virus vorhanden.

Ein Virensuchprogramm besteht grundsätzlich aus zwei Bestandteilen:

- Der **Scanner** ist ein Programm, welches nach bestimmten Vorgaben Datenträger nach Viren durchsucht bzw. diese beseitigt.
- Die **Virendatenbank** enthält Informationen zur Erkennung und/oder Beseitigung von Viren. Die Datenbank muss stets aktuell gehalten werden (nur sinnvoll mit Updateservice), binnen kurzer Zeit ist das Programm ansonsten wertlos.

Eicar - der Test-Virus
Um Virenscanner testen zu können, ohne sich dem Risiko einer Infektion auszusetzen, haben sich Hersteller von Virenscannern auf einen kurzen Code-String geeinigt, der harmlos ist, aber trotzdem von allen Virenscannern als Virus erkannt wird:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Es reicht, ihn in eine Text-Datei zu tippen und die Endung auf *.COM zu ändern, damit der Virenscanner anspringt (siehe auch www.eicar.org).

4.1.2 Einige Virenscanner

60	Bemerkungen	Qualität
VirusScan (NAI/McAfee)	Campuslizenz an der HU	sehr gut
Dr. Solomon’s Anti Virus Toolkit	übernommen durch NAI, Lizenz an der HU ausgelaufen	sehr gut
Anti-Virus (F-Secure)	hoher Preis	gut
Antivir IV/V	hoher Preis	gut

60	Bemerkungen	Qualität
Carmel Turbo Anti Virus (TNT Antivirus)	Entwicklung eingestellt	schlecht
Sophos Anti-Virus	an Hochschulen sehr verbreitet	befriedigend
F-Prot Professional	preisgünstig	sehr gut
Panda Antivirus Platinum		befriedigend
Norton Anti-Virus	verbreitet	gut

Kostenloser Schutz

AntiVir Personal Edition
H+BEDV Datentechnik erlaubt privaten Anwendern unter
http://www.free-av.de
den Download von Antivir 6 für Win9x/ME und NT/2000

F-Prot (DOS)
Bei Data Fellows steht F-Prot unter
http://www.f-prot.com/f-prot/
zum Download bereit.

InoculateIT Personal Edition
http://www.ca.com

Weitere Angebote unter
http://www.heise.de/ct/antivirus/

4.1.3 kurze Programmbeschreibung VirusScan von NAI

VirusScan von NAI enthält folgende Elemente (Auswahl):

Allgemeine Komponenten
Dieser Komponentensatz besteht aus Datendateien und anderen Unterstützungsdateien, die vieleVirusScan-Komponentenprogramme gemeinsam nutzen. Zu diesen Dateien zählen VirusScan-Virusdefinitionsdateien (*.DAT), standardmäßige Konfigurationsdateien sowie weitere Dateien.

VirusScan - Schutz: „On-Demand“
Diese Komponente ermöglicht die uneingeschränkte Kontrolle über die Scanvorgänge. Es können ein Scanvorgang - eine „Scannen auf Anfrage“ genannte Funktion - jederzeit gestartet werden, lokale und Netzwerklaufwerke als Scanziele festgelegt werden, gewählt werden, wie VirusScan auf gefundene Infektionen reagiert, und Berichte über seine Maßnahmen angezeigt werden.

VShield - Schutz: „On-Access“
Diese Komponente bietet einen ständigen Schutz vor Viren, die von Disketten oder aus dem Netzwerk kommen oder in den Speicher geladen werden. VShield startet beim Starten des Computers und bleibt im Speicher, bis er wieder heruntergefahren wird. VShield warnt bei gefundenen Viren, generiert Berichte, die alle seine Maßnahmen zusammenfassen. Die neueste VShield-Version enthält eine Technologie, die vor feindlichen Java-Applets und ActiveX-Steuerelementen schützt. Mit dieser neuen Funktionalität kann VShield E-Mail Nachrichten und Anlagen automatisch scannen, die aus dem Internet über Lotus cc:Mail, Microsoft Mail oder sonstige Mail Clients empfangen werden, die dem Messaging

Application Programming Interface (MAPI) von Microsoft entsprechen. Damit lassen sich ferner feindliche Java-Klassen und ActiveX-Kontrollen herausfiltern, indem die gefundenen mit einer Datenbank von Klassen und Kontrollen, die als schädlich bekannt sind, verglichen werden. Wenn VShield eine Übereinstimmung feststellt, kann es warnen oder schädlichen Objekten automatisch den Zugang zum System verweigern. VShield kann auch verhindern, dass sich der Computer mit gefährlichen Internet-Sites verbindet.

cc:Mail Scan
Diese Komponente enthält eine Technologie, die zum Scannen von Lotus cc:Mail-Mailboxen optimiert wurde, die nicht den MAPI-Standard verwenden.

MAPI-Scanner
Mit dieser Komponente lässt sich die Inbox oder eine sonstige Mailbox für E-Mail-Clientanwendungen nach Bedarf scannen.

WebScanX
Diese Komponente überprüft Dateien, die aus dem Internet heruntergeladen werden, sowie Anlagen von Internet-Mails (erforderlich für cc:Mail) und filtert darüber hinaus gefährliche Java-, Active-X- und Internet-Sites heraus.

VirusScan-Konsole (veraltet auch: VirusScan-Planer)
Mit dieser Komponente können Tasks erstellt werden, die VirusScan durchführen sollen. Eine „Task“ kann alles Mögliche umfassen, wie z. B. das Ausführen eines Scanvorgangs auf einer Reihe von Festplatten zu einer bestimmten Uhrzeit oder in einem bestimmten Intervall oder das Einrichten von VShield zur Ausführung mit bestimmten Optionen.

McAfee ScreenScan
Diese optionale Komponente scannt den Computer, während in Leerlaufzeiten der Bildschirmschoner ausgeführt wird.

Befehlszeilenscanner
Dieser Satz besteht aus SCANPM.EXE, einem leistungsfähigen Scanningagenten für 32-Bit-Umgebungen sowie BOOTSCAN.EXE, einem kleineren speziellen Scanner. Beide Programme ermöglichen die Durchführung von Scanvorgängen in Windows aus dem MS-DOS-Eingabefenster oder der geschützten MS-DOS-Betriebsart heraus. In der Regel wird die grafische Benutzeroberfläche (GUI) von VirusScan zur Durchführung der meisten Scanvorgänge verwendet. Wenn es Probleme gibt, Windows zu starten, oder die VirusScan-GUI-Komponenten in der aktuellen Umgebung nicht ausgeführt werden, kann statt dessen die Befehlszeilenscanner verwendet werden.

Warnmanager (unter Windows NT/2000)
Dieser Windows NT/2000-Dienst empfängt und verteilt Warnmeldungen, die den Benutzer darüber informieren, dass VirusScan einen Virus entdeckt hat.

VirusScan unterstützt die folgenden Plattformen/Betriebssysteme:

- MS-DOS, MS Windows 3.x, MS Windows 9x/ME
- MS Windows NT 3.51/4.0/2000 (Intel/DEC Alpha)
- Mac OS (Apple Macintosh)
- Novell NetWare
- SCO Unix, AIX, HP-UX, Linux, Solaris
- OS/2

Die Humboldt-Universität hat mit der Firma NAI eine Vereinbarung zum unlimitierten Einsatz des Programms am Campus abgeschlossen.

Die Software wird an der HU auf dem Web-Server unter

http://amor.rz.hu-berlin.de/software/nai/

bereitgestellt. Sie kann auch über den DV-Beauftragten der Einrichtung bezogen werden. DAT-Files sind unter

ftp://ftp.hu-berlin.de/pub/mirrors/ftp.nai.com/pub/antivirus/datfiles/4.x

downloadbar.

4.1.4 Installation von VirusScan (am Beispiel von MS Windows 98)

Installation des Programms

- Download und Aufruf von VSC451L.EXE
- Aufruf von setup.exe (Installationsdatei Version 4.5.1)
- Weiter >
- Ich akzeptiere die Lizenzbedingungen - Weiter >
- Benutzerdefinierte Installation - Weiter >
- Scan32 - zwingend notwendig (Scanner-Aufruf)
Systemscan - zwingend notwendig (Grundlagen Systemscan)
E-Mail-Scan - nicht notwendig (für MS Exchange und MS Outlook)
Internetscan - bedingt empfohlen (für JAVA und ActiveX-Sites)
Alarm-Manager - bedingt empfohlen (Alarm-Management)
Screen Scan - bedingt empfohlen
Utility „Virusübermittlung“ - möglich
Utility „Notfalldiskette“ - bedingt empfohlen
Befehlszeilenscanner - empfohlen (Start von der DOS-Eingabeaufforderung)
- Weiter >
- Installieren >
- Konfigurieren >
- Weiter >
- Automatische Aktualisierung jetzt ausführen - Weiter >
- Beenden

Konfiguration DAT-Updates

- Start - Programme - Network Associates - VirusScan-Konsole
- AutoUpdate - Task - Eigenschaften - Konfigurieren
- Hinzufügen
Sitename - HU Berlin
FTP-Verzeichnis - ftp.hu-berlin.de/pub/mirrors/ftp.nai.com/pub/antivirus/datfiles/4.x
Anonymes FTP-Login verwenden - ausschalten
FTP-Login Info... -
Benutzername: ftp
Kennwort: NAI@
Kennwort bestätigen: NAI@
- Network Associates - Bearbeiten - Aktiviert - ausschalten

manuelle Aktualisierung der DAT-Files

- Start - Programme - Network Associates - VirusScan-Konsole -
AutoUpdate - Task - Eigenschaften - Programm - Jetzt ausführen

Empfohlene Einstellungen

- Start - Programme - Network Associates - VirusScan-Konsole - AutoUpdate - Task - Eigenschaften - Zeitplan - Aktivieren - Monatlich

FAQ

- PC „hängt" beim Start von Windows 98
  In der AUTOEXEC.BAT ist die Zeile
  C:\PROGRA~1\NETWOR~1\MCAFEE~1\SCAN.EXE C:\   durch
  C:\PROGRA~1\NETWOR~1\MCAFEE~1\BOOTSCAN.EXE C:\
  auszutauschen.

4.1.5 Anwendungsempfehlungen für VirusScan (am Beispiel von Windows 98)

- Grundsätzlich: Die Virenüberprüfung von Datenträgern sollte, wenn möglich, „**von außen**“ erfolgen (z.B. die Festplatte mit einem Betriebssystem von Diskette), um insbesondere Stealth-Viren keine Möglichkeit zum Verstecken zu geben.

  Aber: Diese Möglichkeit funktioniert nur noch eingeschränkt:
  - Das Betriebssystem auf Diskette (a.A. MS-DOS) muss die Plattenformatierung erkennen (z.B. nicht NTFS)
  - Es werden keine Makroviren, Skript-Viren oder Trojanische Pferde entdeckt.
  - Es ist praktisch unmöglich, die Virendatenbanken aktuell zu halten.
- In regelmäßigen Abständen (etwa wöchentlich) sollte(n) die lokale(n) Festplatte(n) auf Virenbefall überprüft werden.
  Aufruf: Start - Programme - McAfee VirusScan - VirusScan - Scannen in - Netzlaufwerk - Jetzt Scannen
- In regelmäßigen Abständen sollten durch den Administrator mit **VirusScan** (und/oder dem **VirusScan-Planer**) die Netzlaufwerke auf Virenbefall überprüft werden.
  Aufruf: Start - Programme - McAfee VirusScan - VirusScan - Scannen in - Netzlaufwerk - Jetzt Scannen
- An einem Quarantänecomputer sollten unbekannte Disketten mit **VirusScan** vor dem Ersteinsatz auf Virenfreiheit überprüft werden.
  Aufruf: Start - Programme - McAfee VirusScan - VirusScan - Scannen in - A:\ - Jetzt Scannen
- **VShield** sollte installiert und aktiviert werden. Es bietet insbesondere einen Schutz vor Viren aus dem VINES-Netz, dem Internet und von unbekannten Datenträgern.
  Aktivierung: Start - Programme - McAfee VirusScan - McAfee VirusScan-Planer - McAfee VShield - Bei Systemstart

Frage: Was hat es mit dem Killer-Virus „CIH“ auf sich?

Antwort: CIH überschreibt am 26. eines Monats (bei Windows95/98/ME-Rechnern) Teile des Startprogramms im Flash-BIOS und macht damit die Hauptplatine unbenutzbar, verhindert also den Neustart des Rechners. Zusätzlich überschreibt der Virus die Festplatte.
Die Folge: Beim Einschalten „hängt“ der Rechner, noch bevor Text am Bildschirm erscheint. Nur die Festplatte läuft an. Solange der Flash-Baustein nicht ausgetauscht wird, kann der Rechner nicht mehr gebootet werden. CIH ist damit der erste Virus, der es zur Beseitigung seiner Folgen erforderlich macht, den Rechner zu öffnen. Nach dem (kostspieligen) Austausch des BIOS-Bausteins läuft der PC zwar wieder, die Festplatte ist dann aber gelöscht.

Schutzmaßnahmen:
- Falls vorhanden, sollte auf dem Motherboard der Schreibschutz-Jumper aktiviert werden.
- VirusScan von NAI findet und deaktiviert den CIH.

4.2 Makroviren und Skriptviren

4.2.1 Was sind Makro- und Skriptviren?

Ein Virus ist in jeder Programmierumgebung möglich, die folgende Leistungen anbietet:

- Lesen und Schreiben anderer Programme,
- Konstanten und Datenvergleiche,
- Ablaufsteuerung und Fallunterscheidungen.

Die meisten aus der Vergangenheit bekannten Viren benutzten die Programm- (BIOS-, DOS-, Mac-, Unix-) Umgebung des PC und seiner Verwandten, die diese Möglichkeiten bieten.

> Nach einer Studie des Symantec AntiVirus Research Centers (SARC) machen Makroviren nur ca. 13 Prozent der insgesamt bekannten Viren aus, verursachen aber 80 Prozent aller Viren-Schäden.

Viren können aber auch in einer Quellsprache wie Pascal, C, C++, in einer der zahlreichen Skript-Sprachen o.a. formuliert werden. Voraussetzung hierfür ist, dass beim Opferrechner die entsprechende Programmierumgebung zur Verfügung steht und aktiv ist.

Eine günstige Plattform für diese Art Viren sind moderne Anwendungsprogramme, die sowohl eine eigene Programmierumgebung haben als auch in der Nutzung sehr verbreitet sind. Als Medium für die Verbreitung dieserart Viren fungieren die erstellten Dateien (Dokumente), die Programmierumgebung steht mit dem Anwendungsprogramm automatisch zur Verfügung.

Man nennt diese Programmiersprachen Makrosprachen oder Skriptsprachen. Das sind Sprachen, mit deren Hilfe bestimmte Teilaufgaben (insbesondere bei Büroanwendungen) automatisiert werden können. Diese Makrosprachen sind von der jeweiligen Applikation abhängig, es gibt aber auch applikationsübergreifende Sprachen, die in verschiedenen Anwendungsprogrammen lauffähig sind. Ein solcher Quasi-Standard ist beispielsweise das VISUAL BASIC FOR APPLICATIONS (VBA), eine Microsoft-Entwicklung, deren Programme zu allen MS-Office-Produkten (ab der Version 97) kompatibel sind.

Makro- oder Skript Viren können in verschiedenen Programmen auftreten, hier eine Auswahl:

Makroviren	MS Office	Word, Excel, PowerPoint, Access
	weitere Textverarbeitungsprogramme	WordPerfect, AmiPro
	weitere Officeprogramme	StarOffice, QuattroPro
	Grafikprogramme	CorelDRAW
Skriptviren	Mailprogramme	Outlook, Eudora
	Browser	Navigator, Internet Explorer

Die Makrosprachen bieten alle Leistungen, die ein Virenprogrammierer benötigt. Die Häufigkeit der Anwendung stellt einen guten Nährboden für die Verbreitung dar, selbst über unterschiedliche Rechnertypen ist dies möglich. Und sie sind i.A. leicht erlernbar. Ohne tiefe Programmierkenntnisse sind solcherart Viren zu erzeugen.

4.2.2 Makroviren in MS Word

Word bietet ideale Voraussetzungen für die Erstellung und für die rasche und weite Verbreitung von Makroviren. Das hat mehrere Gründe:

- **Jedes** Word-Dokument kann Makros enthalten.
- Bei bestimmten Gelegenheiten startet Word sogenannte *Automakros* ohne explizite Aufforderung durch den Benutzer:
  AUTOEXEC wird beim Start von Word aufgerufen,
  AUTONEW wird beim Anlegen eines neuen Dokuments aufgerufen,
  AUTOOPEN wird beim Öffnen eines Dokuments aufgerufen (besonders gefährlich!),
  AUTOCLOSE wird beim Schließen eines Dokuments aufgerufen,
  AUTOEXIT wird beim Beenden von Word aufgerufen.
- Die **globalen Makros** einer Installation können leicht ergänzt oder verändert werden und stehen bei Bearbeitung beliebiger Dokumente zur Verfügung.
- Die Bedeutung jedes **Menüpunktes** in der Bedieneroberfläche, jeder **Schaltfläche**, sogar jedes **Tastendrucks** kann einfach durch das Bereitstellen eines Makros verändert werden.

In Word wird zwischen lokalen und globalen Makros unterschieden:

- **Lokale Makros** sind in Word-Dokumenten (*.DOC) enthalten und sind damit hauptverantwortlich für die Verbreitung der Viren. Sie stehen nach dem Öffnen eines Dokuments (Datei - Öffnen) zur Verfügung und können aktiv werden.
- **Globale Makros** sind in Dokumentvorlagen (*.DOT) enthalten und werden nach dem Erstellen neuer Dateien (Datei - Neu) aktiviert. Dabei ist meist die Standard-Dokumentvorlage NORMAL.DOT das Opfer von Virenangriffen, welche über Datei - Neu - Leeres Dokument aufgerufen wird.

4.2.3 Schutz vor Makroviren in MS Word

Schutz vor Makroviren in MS Word bedeutet
- die Virenerkennung,
- die Virenbeseitigung und
- die Virenimmunisierung

von *.DOC und *.DOT-Dateien. Dabei sind folgende Hilfsmittel anwendbar:

1 VirusScan: **VirusScan** (!)
Antivirenprogramme (so auch VirusScan von NAI) eignen sich auch zur Erkennung und Beseitigung von Makroviren in *.DOC- und *.DOT-Dateien (vgl. 4.1.5).

2 VirusScan von NAI: **VScan** (!)
Insbesondere VScan ist zur Immunisierung vor Makroviren zu empfehlen. Es werden Makroviren erkannt und beim Abspeichern/Öffnen/Kopieren (fremder) Dokumente entsprechend geschützt.

3 Dokumente von Viren **säubern**
Neben den in Punkt 1 und 2 beschriebenen Möglichkeiten können Dokumente, bei denen man von der Verseuchung weiß, von Makros und damit von Makroviren befreit werden:
Datei - Neu
Einfügen - Datei - name_des_dokuments.doc

4 Änderung der NORMAL.DOT nur nach **Rückfrage** (!)
Diese Funktion wird von vielen Makroviren zwar als erstes mit beseitigt, stellt aber meist einen guten Indikator für einen Virenbefall dar.
Extras - Optionen - Speichern - Automatische Anfrage für Speicherung von Normal.dot

5 NORMAL.DOT mit **Makrovirusschutz** (Version 6.0 bis 7.0) (!)
Dieser Virenschutz hat die gleiche Funktion wie der unter 4 beschriebene, ist aber für die älteren Word-Versionen installierbar. Die Datei SCANPROT.DOT kann vom Microsoft-Server heruntergeladen und in Word eingebunden werden.
Installation über mvtool40.exe, dann Datei - Öffnen - Scanprot.dot

6 NORMAL.DOT mit **Makrovirusschutz** (Version 7.0a bis Version 97) (!)
Diese Funktion warnt bei dem Auftreten von (AutoOpen-)Makros in Dokumenten, unabhängig davon, ob sie von Viren befallen sind oder nicht. Da AutoOpen-Makros in Dokumenten relativ selten sind (wesentlich häufiger treten AutoNew-Makros auf, die in diesem Zusammenhang aber eine geringere Rolle spielen), sollten diese Dokumente vor der Erstbenutzung mit einem Virenscanner überprüft werden. Diese Funktion bietet zusätzlich die Möglichkeit, Dokumente ohne Makros und damit ohne Makroviren zu öffnen.
Extras - Optionen - Allgemein - Makrovirus-Schutz aktivieren

7 NORMAL.DOT mit **Makrovirusschutz** (Version 2000, Version XP) (!)
Makros bzw. deren Quellen können signiert werden, sofern sie als vertrauenswürdig eingestuft werden. Sicherheitsstufen in Word können hoch (nur signierte Makros aus vertrauenswürdigen Quellen dürfen ausgeführt werden, nicht signierte Makros werden automatisch deaktiviert), mittel (Sie können auswählen, ob Sie nicht signierte Makros ausführen möchten) und niedrig (es erfolgt keine Prüfung nach Makros, der Makroschutz ist deaktiviert) definiert werden.
Extras - Makro - Sicherheit...

8 NORMAL.DOT mit **Passwortschutz** (ab Version 97)
Extras - Makro - Visual Basic-Editor - Projekt-Normal - Normal-Eigenschaften - Schutz - Kennwort zum Anzeigen der Projekteigenschaften

9 **Sicherungskopie** der NORMAL.DOT anlegen (!)
Diese (virenfreie!) Sicherungskopie kann die ggf. defekte NORMAL.DOT im Vorlagenverzeichnis ersetzen.

4.3 Maßnahmen bei einem (möglichen) Virenbefall

Wie im dritten Abschnitt beschrieben wurde ein (möglicher) Virenbefall eines Datenträgers festgestellt. Was ist zu tun?

- Erste Reaktion: Ruhe bewahren!
- Es sollten alle aktiven Anwendungen beendet und alle offenen Daten gespeichert werden. Der Rechner sollte neu gestartet werden.
- Mit einem Virenprüfprogramm (wie in 4.1 beschrieben) sollte der Datenträger auf einem möglichen Virenbefall hin überprüft werden.
- Antivirensoftware enthält meist die Funktion der Virenbeseitigung (so auch VirusScan), mit der versucht werden sollte, die Viren zu eliminieren. Es besteht aber dabei die Gefahr, dass ein Virus nicht beseitigt werden kann oder mit der Virenbeseitigung die Datei(en) unbrauchbar wird (werden) (insbesondere bei Programmviren).
- Dateiviren können i.A. durch Löschen derselben beseitigt werden (Achtung: Gelöschte Dateien auch aus dem Papierkorb beseitigen!).
- Besonders hartnäckige Viren lassen sich nur durch Löschen des Datenträgers beseitigen. Dazu sind als erstes alle (virenfreien) Dateien zu sichern (da diese möglicherweise verloren gehen). Dann sollte mit dem Kommando SYS ein neuer Bootsektor auf den Datenträger geschrieben werden. Wenn das nicht ausreicht, ist der Datenträger vollständig neu zu formatieren (Achtung: spätestens jetzt gehen wirklich alle Daten auf diesem Datenträger verloren!).

> Man sollte sich der Gefahr eines Virenbefalls stets bewusst sein, ohne sie überzubewerten. Bei einem vernünftigen Umgang mit dem Computer und Einhaltung der genannten Empfehlungen können die schädlichen Auswirkungen eines Virenbefalls begrenzt werden.

- Bootviren kann man auch mit einem undokumentierten Parameter des FDISK-Befehls vom Datenträger entfernen, der mit der Syntax FDISK/MBR eingegeben wird. Der Nachteil ist, dass dabei mögliche installierte Boot-Manager, die die Spur 0 benötigen, gelöscht werden.
- Abschließend zu einer Virenbeseitigung sollte noch einmal ein vollständiger Virentest mit einem Antivirenprogramm laufen.
- Es sollte versucht werden, die Quelle der Virusinfektion zu ermitteln.
- Weiterhin betroffene Benutzer sollten informiert und gewarnt werden. Auf deren Computer sind die Maßnahmen der Virenerkennung und -beseitigung auszudehnen.
- Der Virenbefall sollte protokolliert und der entsprechende DV-Beauftragte darüber informiert werden.
- Mitarbeiter des Rechenzentrums stehen als Ansprechpartner natürlich gern zur Verfügung.

5 Virenvorsorge

Die Umsetzung einer konsequenten Anti-Virus-Strategie ist ein wirksamer Schutz vor allen Arten von Datenverlusten. Dabei sollten vor allem die folgenden drei Aspekte des Virenschutzes berücksichtigt werden:

- **Vorbeugung** - um die Ausbreitung von Viren einzuschränken.
- **Entdeckung** - um sicherzustellen, dass ein Virus, der in das System eindringen konnte, so rasch wie möglich gefunden wird.
- **Wiederherstellung** - um sicherzugehen, dass Dateien, die verlorengegangen oder beschädigt sind, so rasch wie möglich wiederhergestellt werden können.

Die wichtigsten Einfallstore für Viren (Malware) sind:

> E-Mail-Anhänge, WWW-Downloads, FTP-Downloads, Newsgroups, IRC (Internet Relay Chat), Disketten, CD-ROMs, Dateien im lokalen Netzwerk, Office-Dokumente

Zusammengefasst folgen hier einige Empfehlungen zur Virenvorsorge:

- Sichern Sie regelmäßig alle wichtigen Daten (wenn sie noch virenfrei sind). Legen Sie sich Sicherheitskopien Ihrer wichtigen Daten an.
- Installieren Sie auf Ihrem Rechner eine Antivirus-Software, die im Hintergrund läuft und Ihre Dateizugriffe überwacht.
- Überprüfen Sie regelmäßig Ihre Festplatte mit einem Virenscanner auf Virenbefall. Beachten Sie bitte, dass bei der Virenbeseitigung durch Virenscanner die Gefahr besteht, dass Dateien/Verzeichnisse/Ordner und/oder Bereiche unbrauchbar/gelöscht werden.
- Sorgen Sie dafür, dass der Virenscanner stets aktuell ist.
- Überprüfen Sie unbekannte Datenträger (Disketten) vor Erstbenutzung auf Virenbefall.
- Aktivieren Sie in den Standardanwendungen den Virenschutz für Makroviren (MS Word für Windows ab Version 7.0a, MS Excel und MS Powerpoint jeweils ab Version 97).
- Überprüfen Sie in Mails versandte Dateien vor Erstbenutzung auf Virenbefall. Seien Sie bei Mails von (nicht nur!) unbekannten Absendern besonders vorsichtig.
- Stellen Sie im Windows Explorer folgende Optionen ein:
  - Alle Dateien anzeigen - JA
  - Keine Erweiterungen für ... (bzw.: Dateinamenerweiterung ... ausblenden) - NEIN
  - Verknüpfen Sie *.VBS-Dateien mit dem Notepad:
    im Explorer eine beliebige VBS-Datei anzeigen - Mit Shft+rechter Maustaste Datei anklicken - Öffnen mit ... - Notepad auswählen und „Datei immer mit diesem Programm öffnen“ auswählen - OK
- Öffnen Sie keine Dateien, deren Ursprung nicht zweifelsfrei seriös ist. Dies gilt insbesondere für Dateien aus dem Internet (E-Mail, Newsgroup, IRC, WWW- oder FTP-Download)
- Versenden Sie keine Dokumente, die Sie nicht zuvor auf Makroviren geprüft haben.
- Betreiben Sie kein ungeprüftes „Forwarding“. Leiten Sie keine Mails weiter, deren Inhalt Sie nicht überprüft haben.
- Öffnen Sie keine HTML-formatierten E-Mails, schalten Sie entsprechend Optionen in Ihrem E-Mail-Programm aus (Skript-Viren!).
- Schalten Sie die Option des automatischen Öffnens von Attachment-Dateien in Ihrem Mail-Programm aus. Insbesondere in Microsoft Outlook deaktivieren Sie zusätzlich die Funktion „Automatisches Hinzufügen zum Adressbuch“.
- Gehen Sie als Administrator möglichst nicht ins Internet (Windows NT/2000: Administrator, Unix: root, Novell: supervisor).

- Reduzieren Sie die Zugriffsrechte auf ein Minimum
  als Netzwerk-Administrator: für die Benutzer
  am eigenen PC: Schreibrecht nur in den notwendigen Bereichen
- Arbeiten Sie unter Windows NT/2000 standardmäßig nicht als Administrator, sondern mit einem separaten (in den Rechten eingeschränkten) Benutzerkennzeichen. Bei Administrationsaufgaben loggen Sie sich bewusst als Administrator ein und anschließend wieder aus.
- Versehen Sie Disketten, von denen nur gelesen werden soll, mit dem Schreibschutz. Versehen Sie auch Originalsoftware auf Diskette mit einem Schreibschutz.
- Lassen Sie keine Disketten im Laufwerk stecken, wenn sie nicht benötigt werden.
- Meiden Sie die Benutzung nicht lizenzierter Software, Messe- und Testversionen.
- Legen Sie sich eine virenfreie Bootdiskette zu.

6 Sicherheit in Rechnernetzen

Neben der Virenbekämpfung und -vorsorge sind weitere Sicherheitslöcher bei der Arbeit mit Computernetzen zu beachten:

- Sicherheitsrisiken bei der Benutzung von Computern und Daten (Passwortschutz)
- Sicherheitsrisiken für den lokalen Computer mit aktiven Webseiten (Java-, Javascript-Programme)
- Sicherheitsrisiken bei der Kommunikation (Protokollieren durch Dritte)
- Sicherheitsrisiken bei der Benutzung von E-Mail (Vertraulichkeit, Authentizität, Integrität)
- Sicherheitsrisiken bei der Benutzung personenbezogener Daten (Datenschutz)
- Sicherheitsrisiken bei einer möglichen Softwaresabotage (Eindringen von Schädlingen in die Steuersoftware von technischen Installationen)
  Diese Gefahr besteht sowohl „von außen“ als auch z.b. von eigenen Mitarbeitern.
- Sicherheitsrisiken bei Ausfall von Computertechnik (Hardwaredefekt, Stromausfall, unplanmäßiges Ändern/Löschen von Daten)
  Der Ausfall von Computertechnik kann auch aktiv herbeigeführt werden. Beispielsweise sind sabotierte Halbleiter eine reale Gefahr bei Chip-Herstellern, die bei den Anwendern einen nach einer gewissen Zeit sog. Chip-Infarkt hervorrufen können.

Anhang 1: Verteilung der Viren

(Quelle: Bundesamt für Sicherheit in der Informationstechnik - BSI)

1996

MULTIPART. 6%
SONSTIGE 2%
MAKRO 4%
FILE 5%
BOOT 83%

1997

SONSTIGE 1%
MULTIPART. 6%
MAKRO 32%
BOOT 58%
FILE 3%

1998

SONSTIGE 1%
MULTIPART. 2%
BOOT 48%
MAKRO 47%
FILE 2%

1999

WÜRMER 12%
BOOT 14%
TROJANER 5%
FILE 3%
SONSTIGE 1%
MULTIPART. 1%
MAKRO 64%

2000

BOOT 17%
FILE 1%
WÜRMER 41%
TROJANER 3%
MAKRO 37%
MULTIPART. 1%

2001

BOOT 14%
FILE 1%
WÜRMER 52%
MAKRO 28%
TROJANER 5%

Anhang 2: Einige gute Bekannte

Happy99 ist ein WIN32-Wurm, der als Attachment von E-Mails und über News-Gruppen verbreitet wird. Wird das Programm HAPPY99.EXE aufgerufen, so wird auf dem Bildschirm ein Feuerwerk ausgegeben.

Happy99 erzeugt beim ersten Aufruf zwei Dateien: SKA.EXE und SKA.DLL. SKA.EXE ist eine Kopie von HAPPY99.EXE, die auch SKA.DLL enthält. Anschließend erzeugt Happy99 eine Kopie von WSOCK32.DLL in dem Windows System-Verzeichnis, die den Namen WSOCK32.SKA erhält. Anschließend versucht der Wurm, WSOCK32.DLL so zu ändern, dass die Export-Einträge für zwei Funktionen auf die neue Routine führen. Wird WSOCK32.DLL benutzt, so wird der Registry-Eintrag von RunOnce so geändert, dass SKA.EXE beim nächsten Hochfahren von Windows aufgerufen wird. Wird SKA.EXE ausgeführt, wird kein Feuerwerk angezeigt, sondern Happy99 versucht, WSOCK32.DLL zu manipulieren, solange es nicht ausgeführt wird. In WSOCK32.DLL werden die Exporte "Connect" und "Send" verändert. Dadurch kann der Wurm erkennen, ob der Benutzer aktiv am Netzwerk ist. Wird "Connect" oder "Send" aufgerufen, lädt der Wurm SKA.DLL, das die zwei neuen Export-Einträge "News" und "Mail" enthält. Der Wurm kopiert SKA.EXE in den Speicher, konvertiert es für den Versand mit UUENCODE und sendet es an die vom Benutzer verwendeten Mail-Adresse(n) bzw. News-Gruppen als Attachment Happy99.exe. Der ursprüngliche Header wird unverändert übernommen, die Nachricht enthält aber keinen Inhalt.

Der Wurm enthält folgenden verschlüsselten Text:

Is it a virus, a worm, a trojan?
MOUT-MOUT Hybrid (c)Spanska 1999.

Der Kopf der manipulierten Mail enthält ein neues Feld mit dem Namen "X-Spanska: YES". In der Regel ist dieses Feld allerdings für den Empfänger nicht sichtbar.

Der Datei-Virus **CIH** infiziert Windows EXE-Dateien. Er wird im Speicher resident, wenn ein infiziertes Programm aufgerufen wurde. Anschließend infiziert er jede Windows EXE-Datei, auf die zugegriffen wird. Er gehört also zu den sogenannten "Fast-Infector"-Viren, die sich sehr schnell in PCs ausbreiten.

Der aus Taiwan stammende CIH breitete sich im Juni 1998 über Usenet Benutzergruppen weltweit aus. Anfangs wurde er auch durch Raubkopien einiger Kracker-Untergrundgruppen verteilt. Später waren auf einigen kommerziellen Web-Sites Programme, wie zum Beispiel der beliebte Win Commander, die den CIH enthielten.

Anfang 1999 trat eine Verwirrung bezüglich des Virus-Namens auf. Irgend jemand fand heraus, dass am 26. April der Reaktor-Unfall in Tschernobyl stattfand. Mindestens ein AV-Hersteller warnte deshalb vor einem "neuen" Virus, der den Namen "Tschernobyl" trägt. Dies ist aber nur ein Alias für den CIH v1.2 (CIH.1003).

Vermutlich haben mindestens vier Gruppen, die Lizenzprogramme "knacken" und illegal vertreiben, ungewollt einige der Programme mit dem CIH infiziert und im Sommer 1998 weltweit verbreitet. Zu den infizierten Dateien gehören auch neue Spielprogramme. Ein bisher nicht bewiesene Vermutung ist, das auch illegale Kopien von Windows 98 mit dem CIH infiziert wurden.

Der CIH-Virus enthält eine aggressive Schadfunktion: Er überschreibt, wenn die Schadfunktion ausgelöst wird, den Anfang der Festplatte mit zufälligen Daten. Zusätzlich versucht er, das Flash-BIOS des PCs zu überschreiben. Falls dies möglich ist, kann der PC nicht mehr gestartet werden. Der Inhalt des Flash-BIOS muss erneut geladen werden. Die Flash-Routine setzt einen Pentium Prozessor mit dem Chip-Satz 430TX und verträgliche voraus.

Die meisten Motherboards besitzen einen Jumper, mit dessen Hilfe das Flash-BIOS vor Überschreiben geschützt werden kann. Allerdings muss dieser Jumper meist vom Endbenutzer selbst gesetzt werden.

CIH benutzt für die Infektion eine spezielle Methode, wodurch die Länge der betreffenden Datei nicht verlängert wird. Die Länge des Virus-Codes ist etwa 1 KByte. Er setzt auch spezielle Tricks ein, um Systemaufrufe abzufangen.

CIH kann unter Windows NT/2000 weder aktiv werden noch sich ausbreiten.

Der Makro-Virus **Melissa** wurde das erste Mal am Vormittag des 26. März 1999 in USA gefunden. Er wurde schnell festgestellt, weil er automatisch Mails mit dem Virus-Code mit Hilfe von Outlook abschickt. Der Virus, der ab Office 97 funktionsfähig ist, verbreitete sich mit Hilfe seiner Mail-Funktionen innerhalb weniger Stunden weltweit. Zum Beispiel Microsoft und Intel schalteten ihre Mail-Server ab. Es gibt zwar bereits einige Makro-Viren, die sich automatisch per Mail ausbreiten. Melissa übertrifft diese aber weit. Die Auswirkungen von Melissa in Europa waren verglichen mit USA weitaus geringer. Als der Virus sich in USA ausbreitete, war es in Europa bereits Freitag Abend. Viele europäische Firmen waren am Montag bereits vorgewarnt und konnten eine stärkere Ausbreitung verhindern. Trotzdem berichteten auch deutsche Firmen von Melissa-Infektionen.

Wichtig: Melissa ist unter Microsoft Word 97, Microsoft Word 2000 und Microsoft Outlook E-Mail-Client voll funktionsfähig. Falls auf einem PC Outlook nicht installiert wurde oder keine Internet-Verbindung möglich ist, breitet sich der Virus nur lokal aus, d.h. er infiziert Dokumente und die NORMAL.DOT.

Melissa hat keine programmierte Schadfunktion, durch die permanente Schäden verursacht werden. Lediglich der "Viren-Schutz" von Word wird vom Virus abgeschaltet. Mail-Server großer Unternehmen können allerdings durch eine starke Ausbreitung von Melissa sehr langsam werden oder sogar zusammenbrechen.

Melissa wurde zunächst in der Internet Diskussions-Gruppe alt.sex verbreitet. Der Virus war in einer Datei mit dem Namen LIST.DOC enthalten, die spezielle Passwörter für pornographische Web-Sites enthält. Wenn ein Teilnehmer dieser News-Gruppe die Datei LIST.DOC nach dem Herunterladen mit Word öffnet, wird der Virus ausgeführt und LIST.DOC als Attachment an 50 Adressen aus der Alias-Liste des Benutzers versandt. Der Inhalt dieser Nachricht lautet:

> From: (Name des infizierten Benutzers)
> Subject: Important Message From (Name des infizierten Benutzers)
> To: (50 Namen von der Alias-Liste)
> Here is the document you asked for ... don’t show anyone ;-)
> Attachment: LIST.DOC

Viele Benutzer öffnen ein solches Attachment, weil es von jemand gesandt wurde, den sie kennen. Wichtig: Der Anfang der Alias-Liste von Outlook enthält in vielen Unternehmen Namen von Verteiler-Listen. Dadurch ist die Anzahl infizierter Mails, die von Melissa automatisch abgeschickt werden, sehr viel größer als nur 50. Nachdem der Virus die 50 Mails verschickt hat,

infiziert er Word-Dokumente. Werden diese Dokumente geöffnet, so können diese auch vom Virus versandt werden!

Der Virus wird aktiviert, wenn die Minute gleich dem Tages-Datum ist. Zum Beispiel am 28. März um 8:28, 9:28, 10:28 usw. Der Virus fügt dann den Text:

> Twenty-two points, plus-triple-score, plus fifty points for using all my letters. Game’s over. I’m outta here.

in geöffnete Word-Dokumente ein. Dieser Text, ebenso wie der Alias-Name "Kwyjibo" des Virus-Autors sind der TV-Serie "The Simpsons" entnommen.

PrettyPark ist unter dem Namen **CHV** auch als Trojaner bekannt. Dieses Programm ist sowohl ein Internet-Wurm als auch ein Trojaner, der Passwörter stiehlt. PrettyPark verbreitet sich selbst, indem es seinen Code als Attachment

> Pretty Park.Exe

an Mails anhängt. Wird dieses Programm zum Beispiel durch einen Doppelklick aufgerufen, installiert es sich auf dem PC und sendet E-Mails mit diesem Programm als Attachment. Die Adressen entnimmt es dem im PC gespeicherten Adressbuch. Außerdem informiert es jemand auf einem IRC-Server über das infizierte System und die dort gespeicherten Passwörter. Vermutlich erhält der Autor die gesendeten Informationen auf diesem Weg. Das Programm kann außerdem als Backdoor (Remote Access Control) benutzt werden.

ExploreZip ist ein neuer Wurm, der eine sehr aggressive Schadfunktion besitzt. Der Wurm benutzt für seine Ausbreitung MAPI-Befehle und das Programm Outlook aus Office 97 bzw. Office 2000. Dieser Wurm wurde zuerst am 6. Juni 1999 in Israel gefunden. Inzwischen wurde er auch aus anderen Ländern, zum Beispiel aus Deutschland, Norwegen, USA und Tschechien, gemeldet.

Der Wurm versendet seinen Code per Mail als Attachment mit dem Namen zipped_files.exe. Die Nachricht scheint von einer dem Empfänger bekannten Person zu kommen. Sie enthält folgenden Text:

> Hi [Name des Empfängers]!
> I received your email and i shall send you a reply ASAP.
> Till then, take a look at the attached zipped docs.
> bye

Der Wurm beschafft sich die Namen und Mail-Adressen aus den im infizierten PC eingegangenen Mails.

Das Attachment erweckt den Eindruck, dass es ein ZIP-Archiv ist. Wird das Attachment ausgeführt, wird eine Fehlermeldung in einem Fenster mit folgendem Text ausgegeben, die der von WINZIP gleicht:

> Cannot open file: it does not appear to be a valid archive.
> If this file is part of a ZIP format backup set, insert the
> last disk of the backup set and try again.
> Please press F1 for help.

Der Wurm kopiert sich in das Windows-Verzeichnis mit dem Datei-Namen Explore.exe. Anschließend modifiziert er die Datei WIN.INI, so dass dieses Programm bei jedem Start von

Windows ausgeführt wird. Danach beschafft er sich Mail-Adressen, die er für den Versand seines Codes benutzt.

Benutzt der PC-Anwender nicht Outlook, sondern ein anderes Mail-Programm, so kann sich der Wurm von dessen PC nicht weiter ausbreiten.

Der Wurm enthält zusätzlich eine sehr aggressive Schadfunktion. Er durchsucht alle Laufwerke A: bis Z: und wählt in jedem Laufwerk einige Dateien mit folgenden Extensions aus: DOC, XLS, PPT, ASM, CPP bzw. C.

Die ausgewählten Dateien zerstört er dadurch, dass er die Länge der betreffenden Datei auf 0 setzt. Derartige Schäden können in der Regel nicht restauriert werden.

ExploreZip kann leicht von einem PC entfernt werden:

Die Zeile run=C:\WINDOWS\SYSTEM\EXPLORE.EXE in der Datei WIN.INI löschen.
Die Datei C:\WINDOWS\SYSTEM\EXPLORE.EXE löschen.

Windows beenden und neu starten.

Die Skript-Sprache Corel Script wird von einigen Corel-Produkten, zu denen Corel Draw gehört, eingesetzt. **CSV** ist der erste Virus, der Corel Draw-Dateien infiziert. Der Virus-Code wird in separaten Skript-Dateien abgelegt, die die Extension CSC besitzen. CSV ist ein einfacher Virus, der versucht, alle Dateien im aktuellen Verzeichnis zu infizieren, die die Extension CSC besitzen. Er wird aktiviert, wenn eine infizierte Skript-Datei ausgeführt wird.

Vor der Infektion einer CSC-Datei prüft der Virus, ob diese bereits infiziert ist. Als Kennzeichen benutzt er den Eintrag

REM VIRUS

in der ersten Zeile der Skript-Datei. Existiert dieses Kennzeichen nicht, ändert er zunächst den Namen dieser CSC-Datei in

mallorn.tmp

Anschließend richtet er eine neue Datei ein, die den Namen der zu infizierenden Datei erhält und kopiert den Virus-Code und den Inhalt von mallorn.tmp in diese Datei. Schließlich löscht er die Datei mallorn.tmp.

Der Virus enthält eine Schadfunktion, die am 5. Juni folgenden Text ausgeben soll:

Ai! laurië lantar lassi súrinen!.
Yéni únótime ve rámar aldaron,
yéni ve linte yuldar vánier
mi oromardi lisse-miruvóreva
Andúne pella Vardo tellumar
nu luini yassen tintilar i eleni
ómaryo airetári-lirinen.

Allerdings wird diese Anzeige (durch einen Fehler) nicht im jedem Fall ausgegeben. Der Text stammt aus dem Buch "Lord of the Rings" von J.R.R. Tolkien. Er ist ein Teil von "Galadriel´s Song of Eldamar", der in der Sprache von High elves geschrieben ist. Einige Corel Draw-Dateien können nach der Infektion nicht mehr bearbeitet werden.

Folgende Meldung wird in einem solchen Fall ausgegeben:

Script [Script-Name] contains an error and could not be run.

LoveLetter (Aliase: VBS/LoveLetter , I_Love_You , Lovebug , I-Worm.LoveLetter) ist vom Typ ein VBS-Wurm (Visual Basic Script). Er verbreitet sich über E-Mail als Attachment. LoveLetter wurde das erste Mal am Vormittag des 04. Mai 2000 gemeldet. Er verbreitete sich weltweit innerhalb weniger Stunden. LoveLetter benutzt den Windows Scripting Host (WSH). Dieser Modul kann deinstalliert werden, so dass keine in VBScript geschriebene Programme ausgeführt werden können.
Die E-Mails, die von dem Wurm automatisch versandt werden, besitzen folgende Informationen:

Subject: ILOVEYOU
Body: kindly check the attached LOVELETTER coming from me
Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs

LoveLetter benutzt Outlook für die Verbreitung des Wurms. Er versendet die infizierte E-Mail an alle Adressen aus allen Outlook-Adreßbüchern. Nach dem Versand setzt der Wurm ein Kennzeichen, so dass kein wiederholter Versand erfolgt. Wird das Attachment ausgeführt, kopiert er seinen Code zunächst in das Windows System-Verzeichnis als

MSKernel32.vbs
LOVE-LETTER-FOR-YOU.TXT.vbs

und in das Windows-Verzeichnis als

Win32DLL.vbs.

Anschließend manipuliert er die Registry, so dass er ausgeführt wird, wenn das Windows-System gestartet wird. Folgende Keys werden in die Registry eingefügt:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current\Version\Run\MSKernel32
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current\Version\RunServices\Win32DLL

Danach ersetzt er die Home-Page des MS Internet Explorers durch einen Link auf das Programm

WIN-BUGSFIX.exe

Ist diese Datei vorhanden, wird deren Aufruf auch in die Registry eingetragen. Dadurch wird es bei jedem Neustart von Windows ausgeführt.
Dieses Programm, das der Wurm aus dem Web holt, ist ein Trojaner, der Passworte stiehlt. Beim Start versucht der Trojaner ein verborgenes Fenster zu finden, das den Namen BAROK trägt. Ist dieses vorhanden, wird der Trojaner beendet. Falls es nicht vorhanden ist, wird das Hauptprogramm aktiv. Es prüft in der Registry den Subkey WinFAT32:

HKEY_LOCAL_Machine\Software\Microsoft\Windows\CurrentVersion\Run

Wird der Subkey nicht gefunden, wird er vom Trojaner erzeugt. Er kopiert seinen Code in das Windows System-Verzeichnis als WINFAT32.EXE und ruft es anschließend auf. Durch die Manipulation der Registry wird der Trojaner bei jedem Start von Windows aufgerufen.
Anschließend setzt der Trojaner die Startseite des Internet Explorers auf "about:blank". Er sucht und löscht folgendeRegistry-Einträge:

Software\Microsoft\Windows\CurrentVersion\Policies\Network\
HideSharePwds
Software\Microsoft\Windows\CurrentVersion\Policies\Network\
DisablePwdCaching
.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\
Network\HideSharePwds
.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\
Network\DisablePwdCaching

Danach trägt der Trojaner eine neue Klasse von Fenstern ein und erzeugt ein Fenster, das den Namen BAROK erhält und resident im Speicher als eine verborgene Anwendung bleibt.
Nach dem Systemstart und wenn ein interner Zähler einen gewissen Wert erreicht hat, lädt der Trojaner die Bibliothek MPR.DLL, startet die Funktion WNetEnumCashedPasswords und sendet die gestohlenen RAS-Passworte und alle Windows Passworte an

mailme@super.net.ph
die vermutlich dem Autor des Trojaners gehört. Das Subject der E-Mail ist
Barok... email.passwords.sender.trojan
In dem Code befindet sich folgende Copright Text:
barok ...i hate go to school suck ->by:spyder
@Copyright (c) 2000 GRAMMERSoft Group >Manila,Phils
Außerdem enthält der Code verschlüsselte interne Texte.
Der Wurm generiert eine HTML-Datei
LOVE-LETTER-FOR-YOU.HTM
Diese Datei enthält den Wurm-Code, der per mIRC versandt wird, sobald der PC-Benutzer einen IRC-Channel benutzt.
LoveLetter enthält außerdem einen Virus, der Wirtsprogramme überschreibt. Der Virus sucht nach Dateien auf allen lokalen und Netz-Laufwerken, die bestimmte Extensions besitzen. Er überschreibt diese Dateien mit seinem Code und fügt an den originären Namen zusätzlich die Extension vbs oder vbe an. Dateien, die die Extension
js jse css wsh sct hta
werden gelöscht und eine Datei mit dem gleichen Namen und der Extension vbs erzeugt, die den Wurm-Code enthält.
Dateien, die die Extension
jpg jpeg
werden gelöscht. Eine neue Datei mit dem gleichen Namen und der Extension vbs, die den Wurm-Code enthält, wird erzeugt. Weiterhin werden in gleicher Weise die Dateien mit der Extension
mp3 mp2
zerstört.
Wichtig: Alle Dateien, die vom LoveLetter zerstört wurden, können auf keinen Fall restauriert werden.
Der Virus enthält am Anfang folgenden Kommentar:
rem barok loveletter(vbe)
rem by: spyder / ispyder@mail.com /
@GRAMMERSoft Group (Manila, Philippines
Falls LoveLetter auf einem System durch einen Aufruf des Benutzers installiert wurde, sollte für die manuelle Restaurierung des Systems folgendes ausgeführt werden:
Alle VBS-Dateien auf allen Laufwerken und in allen Verzeichnissen entfernen.
Datei LOVE-LETTER-FOR-YOU.HTM im Windows-Verzeichnis löschen
WIN-BUGFIX.EXE und WINFAT32.EXE im Download-Verzeichnis des Internet Explorer löschen

Eine neue Variante des E-Mail-Wurms "**BadTrans**" verbreitet sich per E-Mail-Attachment. Der Wurm nutzt die bekannte Schwachstelle durch inkorrekte MIME-Header im IE aus, wodurch das Attachment bereits beim Lesen der Mail ausgeführt wird.
Auswirkung:

- Installation des Wurms unter %windir%\INETD.EXE
- Installation des trojanischen Pferdes "Backdoor-NK.svr", welches Passwörter protokolliert und einen Zugang über das Netzwerk ermöglicht
    - %sysdir%\KERN32.EXE bzw. Kernel32.exe oder Kernel.exe (trojanisches Pferd)
    - %sysdir%\HKSDLL.DLL bzw. kdll.dll (Keylogger)
- Übermittlung der IP (des infizierten Systems) an eine wahrscheinlich vom Angreifer kontrollierte IP. (Der Host ist mittlerweile nicht mehr erreichbar.)

- Weiterverbreitung des Wurms durch Anhängen an nicht beantwortete Nachrichten aus dem Outlook-Verzeichnis

Der Wurm "BadTrans" verbreitet sich mittels E-Mail-Attachments, wobei das Subject der Mail leer oder "Re:" ist. Der Wurm nutzt die im März 2001 Schwachstelle bei der Verarbeitung von falschen MIME Types beschriebene Schwachstelle im Internet Explorer 5.x aus, wodurch das Attachment bereits beim Lesen der HTML-E-Mail oder beim Betrachten der (Auto-)Vorschau ausgeführt wird.
Der Attachment-Name wird zufällig aus einer Liste von Dateinamen ausgewählt (z.B. docs.DOC.pif).

- Für den ersten Block des Dateinamen scheinen momentan folgende Varianten vorzuliegen: fun, Humor, docs, info, Sorry_about_yesterday, Me_nude, Card, SETUP, stuff, YOU_are_FAT!, HAMSTER, news_doc, New_Napster_Site, README, images, Pics
- Der zweite Block des Dateinamen setzt sich aus folgenden Möglichkeiten zusammen: .DOC., .MP3., .ZIP.
- Der dritte (und letzte Block) des Dateinamen setzt sich aus folgenden Möglichkeiten zusammen: .pif, .scr

Das Attachment besitzt eine Größe von 13,312 Byte.
Der Wurm legt sich selbst im Windows Verzeichnis als INETD.EXE sowie im Systemverzeichnis als kernel32.exe ab und wird über die Registrierungswerte HKEY_USERS\Software\Microsoft\WindowsNT\CurrentVersion\Windows\RUN=%WinDir%\INETD.EXE sowie HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\Kernel32=kernel32.exe ausgeführt.
Entfernung des Wurms:

- manuelle Entfernung
  - Beenden des Prozess kernel32.exe über den Taskmanager.
  - Löschen Sie die aufgeführten Dateien (siehe Auswirkung) und entfernen Sie die Registrierungsschlüssel HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ RunOnce\kernel32=kern32.exe sowie HKEY_USERS\Software\Microsoft\WindowsNT\CurrentVersion\Windows\RUN=%WinDir%\INETD.EXE
  - Entfernung etwaiger Eintragungen dieser Art in der win.ini
- Entfernung mittels Anti-Virensoftware

Goner ist ein Wurm mit Mass-Mailing-Eigenschaften, der in Visual Basic programmiert wurde. Goner.A wurde das erste Mal am 04.12.2001 gefunden. Er breitet sich als infizierte Outlook E-Mail Message aus. Er nutzt für seine Verbreitung auch den ICQ Instant Messanger, wenn dieser auf dem infizierten System installiert wurde. Er fügt auch einige Scripts in das Verzeichnis von MIRC Clients ein.
Infizierte E-Mails enthalten folgendes:

Subject: Hi
Body: How are you?
When I saw this screen saver, I immediately thought about you
I am in a harry, I promise you will love it!
Attachment: Gone.scr

Wird der Wurm zum Beispiel durch einen Doppelklick aufgerufen, so gibt er eine irreführende Meldung aus:

Error While Analyzing DirectX
About
pentagone
coded by: suid
tested by: THE_SKuLL and Isatan
greetings to: TraceWar, k9-unit, stef16
^Reno
greetings alo to nonick20ut
there where ever

Der Wurm kopiert seinen Code in das Windows System-Verzeichnis und versucht in der Registry einen Startup Key einzutragen. Goner.A holt Adressen aus den Outlook Adressbüchern und versendet an diese infizierte E-Mails. Der Wurm sucht nach folgenden Prozessen und versucht, diese zu beenden: APLICA32.EXE, ZONEALARM.EXE, ESAFE.EXE, CFIADMIN.EXE, CFIAUDIT.EXE, CFINET32.EXE, PCFWallIcon.EXE, FRW.EXE, VSHWIN32.EXE, VSECOMR.EXE, WEBSCANX.EXE, AVCONSOL.EXE, VSSTAT.EXE, PW32.EXE, VW32.EXE, VP32.EXE, VPCC.EXE, VPM.EXE, AVP32.EXE, AVPCC.EXE, AVPM.EXE, AVP.EXE, LOCKDOWN2000.EXE, ICLOAD95.EXE, ICMON.EXE, ICSUPP95.EXE, ICLOADNT.EXE, ICSUPPNT.EXE, TDS2-98.EXE, TDS2-NT.EXE, SAFEWEB.EXE.

Der Wurm versucht, diese Dateien zu löschen. Gelingt ihm dies nicht, manipuliert er die Datei WININIT.INI, so dass diese Dateien beim nächsten Start von Windows gelöscht werden. Außerdem versucht der Wurm das Verzeichnis C:\SAFEWEB zu löschen. Wenn der Wurm mindestens eine der oben gelisteten Dateien gefunden und gelöscht hat, entfernt er seinen Code in dem Verzeichnis, von dem er gestartet wurde, außer wenn dies im Systemverzeichnis von Windows stand.

Anhang 3: Glossar

(nach Network Associates: http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/virus-glossary.asp)

ALIAS: An assumed or alternate name. Some viruses get multiple names since there is no single standard for naming computer viruses.

AVERT: Anti-Virus Emergency Response Team.

Back Door: A feature built into a program by its designer which allows them to gain full or partial access to your system.

Boot Disk: A disk which contains special, hidden, startup files and other programs to run a computer. A boot disk is usually specific to the operating system and version. There are several types of boot disks available to the average user ranging from a standard floppy boot disk to an emergency boot disk or bootable CD. It's important to use a boot disk when disinfecting a computer since most antivirus programs work best when they can gain complete access to the hard drive. In some cases failure to do so will prevent antivirus programs from detecting and removing certain viruses from the computer.

Boot Records: Those areas on diskettes or hard disks that contain some of the first instructions executed by a PC when it is booting. Boot records must be loaded and executed in order to load the operating system. Viruses that infect boot records change them to include a copy of themselves. When the PC boots, the virus program is run and will typically install itself into memory before the operating system is loaded.

Boot Sector Infector: A virus which infects the original boot sector on a floppy diskette. These viruses are particularly serious because information in the boot sector is loaded into memory first, before virus protection code can be executed. A "strict" boot sector infector infects only the boot sector, regardless of whether the target is a hard disk or a floppy diskette. Some viruses always attack the first physical sector of the disk, regardless of the disk type. Additional Information: Top Master Boot Record/Boot Sector Infectors

COM File: COM is short for command, being a file that contains instructions that can do something on your computer. COM files are for DOS based systems and tend to run faster than EXE type programs. Viruses will often infect COM files. When the COM file is run the virus is run as well, often loading it into memory.

Companion Virus: A viral program that does not actually attach to another program, but which uses a similar name and the rules of program precedence to associate itself with the regular program. This kind of virus is also referred to as Spawning.

DDOS (Distributed Denial of Service): A program by this specification is used in a "community network" setting by a controlling program in an effort to initiate an attack known as a "denial of service". DDOS programs receive instruction from a controller program in order to carry out an attack - the attack itself is designed to disable or shutdown the target of the attack.

Denial of Service: A means of attack against a computer, server or network; the attack is either an intentional or an accidental by-product of instruction code which is either launched from a separate network or Internet connected system, or directly at the host. The attack is designed to disable or shutdown the target of the attack.

Dropper: An executable file that, when run, "drops" a virus. A 'Dropper' file has the capability to create a virus and infect the user's system when it is executed. When a 'Dropper' file is scanned, the scan will not detect a virus, because the viral code has not yet been created. The viral code (and virus) is created when the 'Dropper' file is executed.

EICAR: European Institute of Computer Anti-Virus Research has developed a string of characters that can be used to test the proper installation and operation of antivirus software. The EICAR test file is an important file for any serious antivirus software user.

Encryption: A change made to data, code, or a file such that it can no longer be read or accessed without processing (or unencrypting). Viruses may use encryption in order to hinder detection by hiding their viral code. Viruses may also encrypt (change) code or data on a system as part of their payload.

EXE File: EXE, or executable, files are programs that do things on your computer. For example, tank.exe may be a tank game. Files with different extensions, like .dll, are often support files for a program. EXE files are commonly infected by viruses. After infection, the virus is ran each time the program is ran.

False Alarm: Heuristic scans, used to detect new and previously undiscovered viruses, will often give off a lot of false alarms or flags. The novice user may think that a flag during a heuristic scan indicates a virus. In most cases it is just a false alarm but worth checking out nonetheless.

FDOS (Flooder Denial of Service): Similar to DDOS only in the nature of the attack. FDOS programs are singular in form in that there are no other components of the attack structure. FDOS programs can carry out an attack which is generally designed to disable or shutdown the target of the attack.

File Infector: A virus which attaches itself to, or associates itself with, a file. File infectors usually append or prepend themselves to regular program files or overwrite program code. The file-infector class is also used to refer to programs that do not physically attach to files but associate themselves with program filenames. Additional Information: Top File Infecting Viruses

Heuristic: A method of scanning which looks for patterns or activities that are virus like. Most leading packages have a heuristic scanning method to detect new or previously undetected viruses in the wild. The disadvantage of a heuristic scan is that it will often result in a fair number of false alarms or flags.

Hoax: This is usually an email that warns of a non-existant or a valid virus that does more harm in spreading fear.

Hole (as in a "hole" in system memory): When DOS is starting, it begins allocating areas of memory below 640 K, which are used to store information. There are some places where there are gaps in the allocated memory. These gaps are unallocated and unused, and they are considered to be "holes" in system memory. A hole in system memory may also be created in DOS because as DOS loads programs, it often rounds off the amount of memory allocated to the program. For example, a program might need 1025 Bytes (1Kb + 1 Byte). When DOS loads this program, it may allocate 2Kb of memory for the program. Thus 1023 Bytes are actually unused. This unused portion is considered a "hole".

IN-THE-WILD: When a virus is in circulation. Currently about 250 viruses exist in the wild.

Joke Program: This is not a virus, but a program that may bring fear to a user that their hard drive is being formated or their cd tray opens and closes automatically.

Logic Bomb: When a Trojan Horse is left to lie dormant, only to attack when the conditions are just right.

Macro: A saved set of instructions that users may create or edit to automate tasks within certain applications or systems. A Macro Virus is a malicious macro that a user may execute inadvertently and that may cause damage or replicate itself. Additional Information: Macros

Malware (Malicious Software): Programs that are intentionally designed to perform some unauthorized (and often harmful or undesirable) act such as viruses, worms, and trojans.

Master Boot Record (MBR)/Boot Sector Infector: A virus that infects the system's Master Boot Record on hard drives and the Boot Sector on floppy diskettes. This type of virus takes control of the system at a low level by activating between the system hardware and the operating system. A MBR/Boot Sector virus is loaded into memory upon boot-up, before virus detection code can be executed.

Memory Resident: A program that stays in the active RAM of the computer while other programs are running. Accessory software is often of this type, as is activity monitoring and resident scanning software. Viruses often attempt to "go resident". This is one of the functions an activity monitor may check.

Multi-partite Virus: A virus that infects Master Boot Records, Boot Sectors, and Files.

Overwriting Virus: A virus that overwrites infected files. Sometimes used to refer to viruses that overwrite files with garbage data, effectively destroying the data overwritten.

Parasitic: A virus that requires a host to help it to spread.

Payload: The code within a virus that is not part of detection avoidance replication capabilities. The payload code may cause text or graphics to appear on the screen, or it may cause corruption or erasure of data.

Polymorphic: A virus that attempts to evade detection by changing its internal structure or its encryption techniques. Polymorphic viruses change their "form" with each infection in order to avoid detection by antiviral software that scans for signature "forms". Less sophisticated systems are referred to as self-encrypting.

Registry: A database that is used to store instructions and other information. The database is broken down in to keys which values are set for. The alternative to using an INI file in many cases, this Microsoft Windows component is often utilized by virus authors.

Risk Assessment: The calculated measurement of the damage a virus, worm or trojan posses. This assessment is based on several factors including, severity of payload, the number of cases reported, and its ability to spread. Additional Information: Guidelines for the AVERT Risk Assessment (ARA)

Self-Encrypting Viruses: A virus which uses self-encrypting techniques to try to hide its presence. Self-encryption often makes them look more like data within a file rather than the pattern of a virus. This is a stealth technique.

Self-Extracting Files: A file that, when run, extracts itself. Most files transferred across the Internet are compressed to save disk space and lower transfer times. The self-extracting program can extract a virus or Trojan Horse. These types of viruses can be effective since the scanning of compressed files is a rather new technique used by most leading antivirus package. You can not get a virus by just downloading a self-extracting file, you must run it. Always scan new files before using them.

Signature: A series of letters and numbers within the code of a virus which are unique.

Signature File: A database of various virus signatures; the reference used to compare found strings during the disinfection of a computer. Signature files are called a variety of names including the ever-popular DAT file update used by VirusScan. It's important to download or purchase signature file updates often to provide yourself with the best possible protection available to date.

Spawning: A viral program that does not actually attach to another program, but which uses a similar name and the rules of program precedence to associate itself with the regular program. This kind of virus is also referred to as a Companion Virus.

Stealth: A virus that uses one or more of various techniques to avoid detection. A Stealth virus may redirect system pointers and information in order to infect a file without actually changing the infected program file. Another Stealth technique is to conceal an increase in file length by displaying the original, uninfected file length.

System Hang: A complete failure of the operating system. When a program fails, it usually has an opportunity to display an error or diagnostic message. If the entire system fails, such a message will not appear, and input is usually blocked (keystrokes and mouse clicks will be ignored). In the worst cases, the system cannot be restarted without turning the system off completely.

Terminate-and-Stay-Resident: A program that remains active in memory while other programs are run on the system. Examples of TSRs are VShield, a DOS-based mouse, or a CD-ROM driver.

Trigger: An event that a virus writer has programmed the virus to watch for, such as a date, the number of days since the infection occurred, or a sequence of keystrokes. When the trigger event occurs, it activates the virus, which then dispenses its payload.

Trojan Horse: A program that either pretends to have, or is described as having, a set of useful or desirable features, but actually contains a damaging payload. Most frequently the usage is shortened to "Trojan". Trojan Horses are not technically viruses, since they do not replicate.

Tunneling: A virus that avoids standard interfaces to infect files. This allows the virus to infect files without being noticed by a behavior blocker.

Variant: A modified version of an original virus. These modifications can be as simple as a text change, or adding/deleting a few lines of code. It's not uncommon to see a virus changed, and often damaged, by other virus authors over time.

VBS: New method of spreading viruses by using Visual Basic Scripting. Not usually a problem, unless a user has either IE5 or Outlook 98 or higher.

Virus (plural viruses): A software program that attaches itself to another program in computer memory or on a disk, and spreads from one program to another. Viruses may damage data, cause the computer to crash, display messages, or lie dormant.

Worm: This is not technically a virus, but usually spreads via email or irc (Internet Relay Chat).

ZIP File: A file that has been compressed and given the file name extension .zip (usually). Zipped files may contain viruses. Make sure your antivirus program scans for viruses in compressed files.

ZOO Virus: A virus which is only found in virus laboratories and hasn't succeeded in moving into general circulation.